Holst
WORKPLACE CULTURE

DATA PROTECTION POLICY – HOLST

INTRODUCTION

The purpose of this document is to provide a concise policy regarding the data protection obligations of Holst. Holst is a data controller and a data processor with reference to the personal data which it manages, processes and stores.

As the UK Supplier of online systems used for psychometric assessments, Holst has a Model Clause Contract in place with the owners of the online psychometric systems who are sub-processors of the data collected.

RATIONALE

As a data controller and processor, Holst and its staff (hereafter referred-to collectively as Holst) must comply with the data protection rules set out in the relevant UK legislation. This Policy applies to all personal data collected, processed and stored by Holst in the course of its activities.

We collect and process personal information to enable us to provide training to our customers and clients; to promote our services, to maintain our own accounts and records, and to support and manage our employees.

In its role as an employer, Holst may keep information relating to a staff member's physical, physiological or mental well-being, as well as their economic, cultural or social identity.

Personal data also include a combination of identification elements such as physical characteristics, pseudonyms, occupation, home address, etc.

To the extent that Holst's use of personal data qualifies as 'business to customer' processing, including the organisation's communications to its staff members, the organisation is mindful of its obligations under the relevant UK legislation.

SCOPE

The policy covers both personal and sensitive personal data held in relation to its data subjects by Holst. The policy applies equally to personal data held in manual and automated form. All personal and sensitive personal data will be treated with equal care by Holst. Both categories will be equally referred to as personal data in this policy, unless specifically stated otherwise.

DEFINITIONS

For the avoidance of doubt, and for consistency in terminology, the following definitions apply within this Policy.

Data

This includes both automated and manual data.

Automated data means data held on computer, or stored with the intention that it is processed on computer.

Manual data means data that is processed as part of a relevant filing system, or which is stored with the intention that it forms part of a relevant filing system.

Personal Data

Information that relates to a living individual, who can be identified either directly from that data, or indirectly in conjunction with other data which is likely to come into the legitimate possession of Holst.

Sensitive Personal Data

Sensitive personal data is personal data which relates to specific aspects of one's identity or personality, and includes information relating to ethnic or racial identity, political or ideological beliefs, religious beliefs, trade union membership, mental or physical well-being, sexual orientation, or criminal record.

Data Controller

The legal entity responsible for the acquisition, processing and use of the personal data. In the context of this policy; Holst is both a data controller and data processor.

Data Subject

A living individual who is the subject of the personal data, i.e. to whom the data relates either directly or indirectly.

Data Processor

Where Holst is the data controller, the data processor is a person or entity who processes personal data on behalf of Holst on the basis of a formal, written contract, but who is not an employee of Holst.

In the context of this policy, Holst acts as data processor for the data controller (Client) in supplying online psychometric systems.

The owner of the online psychometric system is the data sub-processor.

Data Protection Officer

A person appointed by Holst to monitor compliance with the appropriate data protection legislation, to deal with Subject Access Requests, and to respond to data protection queries from staff members and the general public.

Client

A person or organisation using the services of Holst.

Holst as a Data Controller & Data Processor

In the course of its daily organisational activities, Holst acquires, processes and stores personal data in relation to living individuals. To that extent, Holst is a data controller, and a data processor, and has obligations under the Data Protection legislation, which are reflected in this document.

In accordance with UK Data Protection legislation, this data must be processed fairly and lawfully.

Holst is committed to ensuring that all staff members have sufficient awareness of the legislation in order to be able to anticipate and identify a data protection issue, should one arise. In such

circumstances, staff members must ensure that the Data Protection Officer (DPO) is informed, in order that appropriate corrective action is taken.

Due to the nature of the services provided by Holst, there is a regular and active exchange of personal data between Holst and its data subjects. In addition, Holst exchanges personal data with data processors on the data controllers' and data subjects' behalf. This is consistent with Holst's obligations under the terms of its contracts with its data processors and sub processors.

This policy provides the guidelines for this exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with the Data Protection Officer to seek clarification.

THIRD-PARTY PROCESSORS

In the course of its role as data controller, Holst engages third-party service providers, or data processors, to process personal data on its behalf.

In each case, a formal, written contract is in place with the processor, outlining their obligations in relation to the personal data, the security measures that they must have in place to protect the data, the specific purpose or purposes for which they are engaged, and the understanding that they will only process the data in compliance with the UK Data Protection legislation.

The contract also includes reference to the fact that the data controller is entitled, from time to time, to audit or inspect the data management activities of the data processor, and to ensure that they remain compliant with the legislation, and with the terms of the contract.

THE EIGHT DATA PROTECTION PRINCIPLES

The following key principles are enshrined in UK legislation and are fundamental to Holst's data protection policy.

1. **Fair and Lawful**: Personal data is processed fairly and lawfully:
    - For data to be processed fairly, a data controller must:
    - have legitimate grounds for collecting and using the personal data;
    - not use the data in ways that have unjustified adverse effects on the individuals concerned;
    - be transparent about the intention to use the data, and give individuals appropriate privacy notices when collecting their personal data;
    - handle people's personal data only in ways they would reasonably expect; and
    - ensure they do not do anything unlawful with the data.

Holst meet this obligation in the following way:

- Where possible, the informed consent of the data subject is sought before their data is processed;
- Where it is not possible to seek consent, Holst ensure that collection of the data is justified under one of the other lawful processing conditions – legal obligation, contractual necessity, etc.;
- Processing of the personal data is carried out only as part of Holst's lawful activities, and it safeguards the rights and freedoms of the data subject;
- The data subject's data is not disclosed to a third party other than to a party contracted to Holst and operating on its behalf, or where Holst is required to do so by law.

2. **Purposes**: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes:

Holst meet this obligation in the following way:

- Holst obtain data for purposes which are specific, lawful and clearly stated.
- A data subject has the right to question the purpose(s) for which Holst holds their data, and Holst is able to clearly state that purpose or purposes.

3. **Adequacy**: Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

Holst meet this obligation in the following way:

- Holst ensures that the data it processes in relation to data subjects are relevant to the purposes for which the data are collected.
- Data which are not relevant to such processing are not acquired or maintained.

4. **Accuracy**: Personal data shall be accurate and, where necessary, kept up to date.

Holst meet this obligation in the following way:

- Ensuring that administrative and IT validation processes are in place to conduct regular assessments of data accuracy;
- Conducting periodic reviews and audits to ensure that relevant data is kept accurate and up-to-date. Holst conducts a review of sample data every six months to ensure accuracy;
- Ensuring that staff contact details and details on next-of-kin are reviewed and updated every two years, or on an 'ad hoc' basis where staff members inform the office of such changes;

- Conducting regular assessments in order to validate the need to keep certain personal data.

5. **Retention**: Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes

As a data controller, Holst must:

- review the length of time personal data is retained;
- consider the purpose or purposes for holding the information and in deciding whether (and for how long) to retain it;
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date.

Holst meet this obligation in the following way:

- If data is being retained indefinitely, a justification is provided;
- Once the respective retention period has elapsed, Holst undertakes to destroy, erase or otherwise put this data beyond use;
- Data is destroyed as per the Data Destruction Policy in place at Holst;
- Access to, and management of, staff and customer records is limited to those staff members who have appropriate authorisation and password access.

6. **Rights**: Personal data shall be processed in accordance with the rights of data subjects under this Act.

As a Data Controller and Data Processor, Holst has the following obligation:

- A right of access to a copy of the information comprised in their personal data; a right to object to processing that is likely to cause or is causing damage or distress;
- A right to prevent processing for direct marketing;
- A right to object to decisions being taken by automated means;
- A right in certain circumstances to have inaccurate personal data rectified, blocked, erased or destroyed; and
- A right to claim compensation for damages caused by a breach of the Act.

Holst meet this obligation in the following way:

- A Subject Access Request procedure is in place;
- A mechanism is in place to capture data subject preferences;

- If using Direct Marketing, we ensure Opt-ins and Opt outs are as per current data protection legislation;
- If using Profiling, we ensure the data subject is aware that they are being profiled and have the opportunity to object to such activity;
- We have mechanisms in place to capture communication from data subjects that refer to amending their personal data;
- We agree to pay in the instance where compensation has been awarded for breach of the Act.

7. **Security**: Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

- Holst meet this obligation in the following way:
- Holst use a risk based approach to security of data. The level of security in place shall commensurate with the level of risk to security of the data;
- Holst employ high standards of security in order to protect the personal data under its care;
- Holst's Password Policy and Data & Destruction Policies guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Holst in its capacity as data controller;
- In the event of a data security breach affecting the personal data being processed on behalf of the data controller, the relevant third-party processor notifies the data controller without undue delay;
- Jo Emmerson of Holst is responsible for ensuring information security.

8. **International**: Personal data shall not be transferred to a country or territory outside the EEA unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Holst meet this obligation in the following way:

- Assess whether or not the data can be anonymized prior to transfer;
- Map the process to clearly establish if the data transits through the non-EEA country or is the data actually processed in the non EEA country;
- Ensure that there is no personal data whatsoever on the website;

- Establish if the destination country is on the EU Commission's list of countries or territories who provide adequate protection for the rights and freedoms of data subjects. Personal data may be shared with country's on this list;
- In any case, we undertake to map the transfer process to establish the risks to personal data that may arise. We undertake to mitigate those risks to an acceptable risk level prior to transfer by means of adequate safeguards:
    - Adequate safeguards include Model Contract Clauses, Binding Corporate Rules, or other contractual arrangements;
    - Where "adequate safeguards" are established, the rights of data subjects continue to be protected even after their data has been transferred outside the EEA.

IMPLEMENTATION

As a data controller and processor, Holst ensures that any entity which processes personal data on its behalf (a data processor) does so in a manner compliant with the Data Protection legislation through a formal Data Processor Agreement.

Regular audit trail monitoring will be done by the Data Protection Officer to ensure compliance with this Agreement by any third-party entity which processes personal data on behalf of Holst. Failure of a data processor to manage Holst's data in a compliant manner will be viewed as a breach of contract, and will be pursued through the courts. Failure of Holst's staff to process personal data in compliance with this policy may result in disciplinary proceedings.